Torbay and South Devon NHS Foundation Trust

Personal Device Use Policy

Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Date of Issue:	April 2026	Next Review Date:	July 2027
Version:	1	Last Review Date:	
Author:	Information Governance Officer		
Director Responsible	Chief Nurse		
Approval Route: IM&T Group			
Approved By:		**Date Approved:**	
Information Governance Operational Group			
IM&T Group		19 March 2026	
Links or overlaps with other policies:			
• Code of Conduct for employees in respect of confidentiality • Information Asset Management Policy, Procedure and Guidance • Information Governance Policy • Information Management and Technology Security Policy • Mobile Phone Policy • Offsite Computing Policy • Password Policy • Network User Security Operating Policy			
We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership. We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
1	Final	March 2026	New Policy	IM&T Group, 19 March 2026

Contents

1. Introduction

1.1. The purpose of this policy is to define the limited and controlled circumstances under which personal devices (also known as Bring Your Own Device – BYOD) may be used to access Trust systems, in order to protect patient confidentiality, organisational data, and Trust systems from information security risks.

1.2. This policy supports and should be read in conjunction with:

- Microsoft 365 Usage Policy
- Mobile Phone Policy
- Network User Security Operating Policy

2. Scope

2.1. This policy applies to all personally owned smartphones, tablets, and computers.

2.2. This policy applies to any employees, Contractors and sub-contractors, Agency and Bank staff; and Board, Committee, sub-committee and advisory group members using a personal device to access Trust systems, whether on or off Trust premises.

2.3. This policy does not apply to Trust owned or Trust managed devices.

3. Permitted use of personal devices

3.1. Personal devices may only be used for the following purposes:

a) Access to the Trust's Microsoft 365 environment, including email, calendars, and collaboration tools, in line with the Microsoft 365 Usage Policy

b) Access to the Epic Electronic Patient Record (EPR) via Haiku or Canto where the user has been explicitly authorised to do so by the Trust's Epic Role Based Access Controls (RBAC).

3.2. No other Trust systems, applications, or data repositories may be accessed from personal devices unless formally approved through Trust governance processes.

3.3. All use must be strictly necessary for work purposes and abide by the Trust's human resources and information governance policies.

4. Responsibilities of staff using personal devices

4.1. All users accessing Trust systems via personal devices must:

- Comply with this policy and all related Trust policies
- Inform the Trust of any lost / stolen devices or suspected compromise or unauthorised access
- Cease using personal devices for Trust access if the device becomes non-compliant

4.2. Failure to comply may result in removal of access and further action under Trust disciplinary procedures.

5. Prohibited use of personal devices

5.1. The following activities are strictly prohibited on personal devices:

- Accessing Epic via any method other than Haiku or Canto
- Downloading, storing, or caching Trust or patient data locally on the device
- Using personal devices as a primary or sole method of accessing patient identifiable data
- Jailbreaking, rooting, or otherwise bypassing manufacturer security controls
- Circumventing Trust security controls or conditional access policies

5.2. Any breach may result in withdrawal of access and disciplinary action as per the Trust's Disciplinary Policy.

6. Personal device security and configuration

6.1. Any personal device used to access Trust systems must meet the following minimum-security requirements:

6.1.1. Device Ownership and Use

- The device must not be shared with any other person (this includes children, family members, friends, or carers)
- The user remains fully accountable for all activity conducted on the device

6.1.2. Authentication and Access Controls

- Devices must be protected by:
- A secure device passcode, PIN, biometric control, or equivalent
- Access to Microsoft 365, Epic Haiku, or Epic Canto must:
  - Use the individual's own account only
  - All app use must be protected by Multi Factor Authentication (MFA) at all times
- Credentials must never be shared or stored insecurely.

6.1.3. Operating System and Patch Management

- Devices must be:
  - Running a vendor supported operating system
  - Fully updated to the latest available OS and security patch level
  - Devices that are no longer receiving manufacturer security updates must not be used.

7. Device compliance and monitoring

7.1. The Trust reserves the right to:

- Enforce conditional access controls
- Block access from non-compliant or insecure devices
- Require re-authentication or re-validation of devices
- Withdraw personal device access at any time where risk is identified

7.2. Use of personal devices for Trust systems may be monitored in accordance with Trust policies and applicable legislation.

8. Discouraged device brands and models

8.1. To reduce cyber security risk, the Trust strongly discourages the use of certain personal device brands and models that present increased risk due to declining manufacturer support, delayed security updates, or known security concerns.

8.2. As of 2026, this includes (but is not limited to):

- Older Samsung models (no longer receiving timely OS or security updates)
- Older Xiaomi / Redmi / Poco models
- Huawei devices
- ZTE devices
- UMX devices

8.3. Devices from these manufacturers or product ranges may be blocked from accessing Trust systems if they do not meet minimum security and update requirements.

8.4. Devices which are end of life and no longer receiving security updates are not appropriate for use.

8.4.1. Devices can be checked by using

- https://endoflife.date/android
- https://endoflife.date/apple

9. Training

9.1. All staff will attend, as part of their induction, training sessions on Information Governance and additional annual training will be provided to all staff through a mandatory training online or face-to-face programme.

9.2. All staff accessing Epic must complete mandatory Epic Information Governance training prior to accessing the environment via Haiku or Canto.

10. Monitoring and review

10.1. This policy will be reviewed on an annual basis by the IM&T Group and monitored by the Cyber Security Team.

11. Distribution

11.1. This policy document will be made available to staff via ICON, the Trust Website and signposted in the Staff Bulletin.

11.2. Awareness will be raised through Equality Impact Assessment training, all ratifying committees/groups, policies and procedures training and ICON.

12. Key Contacts

Contact	Email	Phone
Data Protection Officer	Tsdft.dpo@nhs.net	07393 799539
Information Governance Team	tsdft.igteam@nhs.net	01803 654868
Caldicott Guardian	tsdft.caldicottguardian@nhs.net	
Cyber Security	Tsdft.cybersecurity@nhs.net	
Microsoft 365 Team	Tsdft.microsoft365@nhs.net	

13. Appendices

Appendix 1: Rapid Equality Impact Assessment

Torbay and South Devon NHS Foundation Trust

Appendix 1
Rapid Equality Impact Assessment *(for use when writing policies and procedures)*

Policy Title (and number)	***Personal Device Use Policy***	**Version and Date**	*1*
Policy Author	Information Governance Officer		

An equality impact assessment (EIA) is a process designed to ensure that a policy, project or scheme does not discriminate or disadvantage people. EIAs also improve and promote equality. Consider the nature and extent of the impact, not the number of people affected.

EQUALITY ANALYSIS: How well do people from protected groups fare in relation to the general population?
PLEASE NOTE: Any 'Yes' answers may trigger a full EIA and must be referred to the equality leads below

Is it likely that the policy/procedure could treat people from protected groups less favorably than the general population? (see below)

Age	Yes ☐ No☒	Disability	Yes ☐ No☒	Sexual Orientation	Yes ☐ No☒
Race	Yes ☐ No☒	Gender	Yes ☐ No☒	Religion/Belief (non)	Yes ☐ No☒
Gender Reassignment	Yes ☐ No☒	Pregnancy/ Maternity	Yes ☐ No☒	Marriage/ Civil Partnership	Yes ☐ No☒

Is it likely that the policy/procedure could affect particular 'Inclusion Health' groups less favorably than the general population? (substance misuse; teenage mums; carers[1]; travellers[2]; homeless[3]; convictions; social isolation[4]; refugees)	Yes ☐ No☒
Please provide details for each protected group where you have indicated 'Yes'.	

VISION AND VALUES: Policies must aim to remove unintentional barriers and promote inclusion

Is inclusive language[5] used throughout?	Yes ☒ No☐
Are the services outlined in the policy/procedure fully accessible[6]?	Yes ☒ No☐
Does the policy/procedure encourage individualised and person-centered care?	Yes ☒ No☐
Could there be an adverse impact on an individual's independence or autonomy[7]?	Yes ☐ No☒
If 'Yes', how will you mitigate this risk to ensure fair and equal access?	

EXTERNAL FACTORS

Is the policy/procedure a result of national legislation which cannot be modified in any way?	Yes ☐ No☒
What is the reason for writing this policy? (Is it a result in a change of legislation/ national research?)	
To facilitate a standardized approach to policy documents across the Trust	
Who was consulted when drafting this policy/procedure? What were the recommendations/suggestions?	

ACTION PLAN: Please list all actions identified to address any impacts

Action	Person responsible	Completion date

AUTHORISATION:
By signing below, I confirm that the named person responsible above is aware of the actions assigned to them

Name of person completing the form	**Information Governance Officer**	**Signature**	
Validated by (line manager)	**Data Protection Officer**	**Signature**	

Any issues Please contact Diversity & Inclusion Lead
For Torbay and South Devon NHS Trusts, please email tsdft.diversityandinclusion@nhs.net

[1] Consider any additional needs of carers/ parents/ advocates etc, in addition to the service user
[2] Travellers may not be registered with a GP - consider how they may access/ be aware of services available to them
[3] Consider any provisions for those with no fixed abode, particularly relating to impact on discharge
[4] Consider how someone will be aware of (or access) a service if socially or geographically isolated
[5] Language must be relevant and appropriate, for example referring to partners, not husbands or wives
[6] Consider both physical access to services and how information/ communication in available in an accessible format
[7] Example: a telephone-based service may discriminate against people who are d/Deaf. Whilst someone may be able to act on their behalf, this does not promote independence or autonomy